UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Records and information associated with the cellular device assigned IP Address 2607:fb90:d222:4d8d:b933:527f:26c3:698f, that is in the custody or control of T-Mobile, more fully described in Attachment A

Case No. 21-898M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☐ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1073	Unlawful Flight to Avoid Prosecution

The application is based on these facts:

see affidavit.

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of 90 days *(give exact ending date if more than 30 days:* 10/14/2021 *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Ryan Carpenter, TFO USMS

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 06/16/2021

Judge's signature

City and state: Milwaukee, WI

Nancy Joseph, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Police Officer Ryan Carpenter, being first duly sworn, hereby depose and state as follows:

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c)(1)(A), for information about the location of the cellular telephone assigned IP Address: **2607:fb90:d222:4d8d:b933:527f: 26c3:698f,** which was used at multiple times listed in Attachment A on June 8, 2021 (the "**Target Cell Phone**"), whose service provider is T-Mobile ("Service Provider"), a wireless telephone service provider headquartered at 4 Sylvan, Parsippany, NJ 07054. The **Target Cell Phone** is described herein and in Attachment A, and the location information to be seized is described herein and in Attachment B.

2. Because this warrant seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a "pen register" and/or "trap and trace device," see 18 U.S.C. § 3127(3) & (4), the requested warrant is designed to also comply with the Pen Register Act. See 18 U.S.C. §§ 3121-3127. The requested warrant therefore includes all the information required to be included in an order pursuant to that statute. See 18 U.S.C. § 3123(b)(1).

3. I am a Task Force Officer (TFO) with the United States Marshals Service, and I have been employed full time as a Police Officer with the Milwaukee Police Department for over 19 years. One of my primary duties is to investigate and

arrest state and federal fugitives. Your affiant is assigned to the U.S. Marshals Fugitive Task Force and has been since August 2020. Prior to being assigned to the U.S. Marshals Task Force, your affiant was assigned to the Fugitive Apprehension Unit of the Milwaukee Police Department for over ten years. Your affiant has been involved in thousands of fugitive investigations during this period. Many of these investigations were aided by procurement of records related to electronic communications and subsequent analysis of those records. In most of those cases, the records provided critical investigative leads and corroborative evidence. I have had previous experiences using electronic location data to locate and apprehend fugitives.

4. I am an investigator or law enforcement officer of the United States within the meaning of 18 U.S.C. Section 2510(7), in that I am empowered by law to conduct investigations.

5. The facts in this affidavit come from my training and experience, my review of documents and information obtained from other agents. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on the facts set forth in this affidavit, there is probable cause to believe that Bengi J. PENA-GOMEZ has violated 18 U.S.C. § 1073 (Unlawful Flight to Avoid Prosecution) and is the subject of an arrest warrant issued on March 5, 2021. There is also probable cause to believe that the information described in Attachment B will assist law enforcement in arresting PENA-GOMEZ, who is a "person to be arrested" within the meaning of Federal Rule of Criminal Procedure

41(c)(4).

JURISDICTION

7. The court has jurisdiction to issue the proposed warrant because it is a "court of competent jurisdiction" as defined 18 U.S.C. Section 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. Section 2711(3)(A)(i).

PROBABLE CAUSE

8. On August 10, 2020, a criminal complaint was issued in Milwaukee County Circuit Court, case number 2020CF002727, charging PENA-GOMEZ with one count of First Degree Intentional Homicide, contrary to Wis. Stat. §§ 940.01(1)(a) and 939.50(3)(a). An arrest warrant (warrant number K01164) was issued the same day. The charge of First Degree Intentional Homicide is a Class A Felony punishable by life imprisonment.

9. The criminal complaint alleges that on August 1, 2020, PENA-GOMEZ was operating a white 2008 Ford Escape and driving westbound along the 1700 block of W. Mitchell Street, when he abruptly swerved into the opposite lane of traffic, which caused a collision with a moped that was driving in the eastbound direction. The collision caused JCP, the operator of the moped, to be ejected from the moped. Both vehicles ended up on the sidewalk along the south side of the street. PENA-GOMEZ exited the driver's side of the Ford Escape and fled the scene without checking on JCP. A law enforcement officer reviewed video surveillance obtained from a nearby church and compared the driver of the white Ford Escape to booking photographs of PENA-GOMEZ. This review led officers to positively

identify PENA-GOMEZ as the operator of the vehicle that struck JCP on the moped. The complaint also explains that the Ford Escape registered to PENA-GOMEZ's address on W. National Avenue in Milwaukee, Wisconsin.

10. According to the criminal complaint, JCP was taken to the hospital where he later died. An autopsy concluded that his death was caused by crushing blunt force injuries to his torso, specifically his bowels and spleen. The autopsy further revealed that JCP suffered internal bleeding and a lot of brain swelling, another likely cause of death.

11. The complaint further explains that law enforcement officers thereafter interviewed PENA-GOMEZ's mother, GCP, who stated that her son called her after the accident to tell her that he tracked down the man that shot him in 2019, that he followed the victim through the Puerto Rican fest, that he intentionally crashed into the victim head on, and that he was going to shoot the injured victim but was unable to do so because of the bystanders gathered around JCP. On August 2, 2020, officers searched PENA-GOMEZ's house pursuant to his girlfriend's consent. Upon the search, officers located clothing worn by PENA-GOMEZ in the video footage. They further recovered three unfired ammunition cartridges. A search of the white Ford Escape revealed an AR-15 rifle in the cargo area containing a 100-round drum magazine. The safety selector switch of the firearm was set to FIRE.

12. On October 30, 2020, the Milwaukee Police Department requested the assistance of the U.S. Marshals Great Lakes Regional Fugitive Task Force of the Eastern District of Wisconsin to assist with the apprehension of PENA-GOMEZ, as

it was believed that PENA-GOMEZ fled the state of Wisconsin.

13. According to MPD reports related to the homicide investigation for which PENA-GOMEZ is charged, PENA-GOMEZ, has a child-in-common with an individual identified as Johannie Soto-Camacho (Soto-Camacho).

14. On November 2, 2020, an active Facebook account was located for Soto-Camacho using an open source search of Facebook.com. The account located is under the url: https://m.facebook.com/johannie.soto.1, and has a screen name of "Johannie Soto Camacho." I was able to identify the account as being Soto-Camacho's by comparing the Wisconsin Department of Transportation photograph of Soto-Camacho to the photos depicted in the publicly displayed photos within this account.

15. On November 9, 2020, a warrant was obtained and served to Facebook regarding the account "Johannie Soto Camacho." Information from Facebook was returned on December 7, 2020. Those records included approximately 7,064 pages of information, including private messages between Soto-Camacho and other Facebook users.

16. Soto-Camacho's lawfully obtained Facebook messages reflect that PENA-GOMEZ intended to travel from Milwaukee, Wisconsin, to the area of Atlanta, Georgia.

17. For example, on August, 3, 2020, at approximately 9:58 p.m. CST, which was two days after the homicide involving PENA-GOMEZ, Soto-Camacho sent a private Facebook message to https://www.facebook.com/neyshanicole.penagomez/ (FB ID: 1285596827), a

Facebook account believed to be a family member of PENA-GOMEZ. The message stated: "But we'll get him out of here for Atlanta." Law enforcement officials believe that Soto-Camacho was referring to getting PENA-GOMEZ out of Milwaukee to Atlanta.

18. On August 3, 2020, at 12:40 p.m. CST., Soto-Camacho sent a private Facebook message to "Leixpo Ohcamac, a Facebook account believed to be a family member of hers. (FB ID: 100049061476637). The message stated: "I only ask that you get Bengi (PENA-GOMEZ) out of there as soon as possible." A few minutes later, "Leixpo Ohcamac" [Facebook account user name] replied: "…he is fine and we are going to take him to Atlanta with other papers."

19. On August 4, 2020, at 10:16:32 p.m.CST, Soto-Camacho received a private Facebook message from Facebook account user https://www.facebook.com/emi.camacho1988/, a Facebook account belonging to a family member of hers (FB ID:100002153124834). The message stated: "…and by Pipito everything is fine?" Soto-Camacho replied that same day, stating: "He's fine so far on Friday we get him out of Milwaukee." Law enforcement officials believe based upon the context of the messages that "Pipito" is a reference to PENA-GOMEZ.

20. On August 8, 2020, at 7:49 a.m. CST, Soto-Camacho sent a private message to https://www.facebook.com/emi.camacho1988/, a Facebook account of a family member of hers (FB ID: 100002153124834) The message stated: "today they look for him at night to take him to Atlanta."

21. Since August 10, 2020, Bengi PENA-GOMEZ has avoided law enforcement apprehension and remains at large, despite efforts of MPD and the

United States Marshals Service to locate and arrest him.

22. On March 5, 2021, United States Magistrate Judge Nancy Joseph authorized a criminal complaint charging PENA-GOMEZ with unlawfully fleeing to avoid prosecution. *See* 21-810M(NJ). An arrest warrant was issued that same day.

PENA-GOMEZ Facebook Account

23. The affiant was able to identify a Facebook account under the name as "Pito Glock" and identified as https://facebook.com/joe.london.144 ; FB ID: 100065636080914. The page is open to the public, and while examining the page, there is viewable communication between the person controlling that account and an account known to be controlled by Johannie Soto-Camacho.

24. On June 2, 2021, Milwaukee County Circuit Court Judge Rebecca Kiefer authorized a warrant for content from the Facebook page https://facebook.com/joe.london.144 ; FB ID: 100065636080914 with the screen name "Pito Glock." The records from that warrant were returned from Facebook on June 11, 2021.

25. The affiant has personally reviewed those records and discovered communication between the account "Pito Glock" and the account "Johannie Soto Camacho," held by Johannie Soto-Camacho, which the affiant knows to be the person with whom PENA-GOMEZ has two children in common. The communication between the accounts was time stamped on May 25, 2021, 12:32:40 (UTC) and contained the following message:

> "Johannie Soto Camacho porq borras mis comentarios ? yo solo quiero aclararle al q piense estar contigo q si al papa de tus hijos se las pegabas con 10 mas tu se las pegas a cualquiera y luego te haces la mas santa senda putipuerka es lo q

> eres por esp YO q soy el padre de tus hijos no quiero estar contigo y te mande pal carajo por puta"

25. According to the translator application Google Translate, the above message contained the following message:

> "Johannie Soto Camacho, why do you delete my comments? . . . because I am the father of your children I do not want to be with you and I sent you to hell for a bitch"

26. Additionally, the affiant observed in this account multiple pictures of an individual that I know and believe to be PENA-GOMEZ, based upon a review of photographs in which PENA-GOMEZ is positive identified.

27. Therefore, based on a review of this Facebook account, the affiant believes that Bengi J. PENA-GOMEZ is controlling the Facebook account https://facebook.com/joe.london.144 ; FB ID: 100065636080914 with the screen name "Pito Glock."

28. On June 3, 2021, an order was signed by the Honorable Nancy Joseph, Eastern District of Wisconsin authorizing the installation and use of pen register and trap and trace on the account https://facebook.com/joe.london.144 ; FB ID: 100065636080914.

29. That order was served on Facebook, and on Monday, June 7, 2021, the affiant began receiving IP addresses associated with account activity related to the account https://facebook.com/joe.london.144 ; FB ID: 100065636080914. Between the date of installation of the pen register to the current date it was discovered that PENA-GOMEZ was consistently utilizing IP addresses associated with a T-Mobile cellular device. The most recent IP used is **2607:fb90:d222:4d8d:b933:527f:26c3:698f**, which was used on June 8, 2021, seventeen times.

30. Based on the consistent usage of a T-Mobile IP address it is believed that locating the associated device will reveal the location of PENA-GOMEZ.

TECHNICAL BACKGROUND: DYNAMIC IP ADDRESSES

31. Your affiant used the website www.arin.net, the "American Registry of Internet Numbers (ARIN)," to obtain the owner and operator of the IP address mentioned previously: **2607:fb90:d222:4d8d:b933:527f:26c3:698f**, which was used at multiple times listed in Attachment A on June 8, 2021. According to ARIN, the listed IP address is owned and operation by T-Mobile. Your affiant has used ARIN in the past and knows this website to be reliable.

31. Based on training and experience, I know that T-Mobile is a cellular service provider and does have the ability to connect their cellular service to the internet through Dynamic Internet Protocols. A dynamic Internet Protocol address (dynamic IP address) is a temporary IP address that is assigned to a computing device or node when it's connected to a network. A dynamic IP address is an automatically configured IP address assigned by a Dynamic Host Configuration Protocol (DHCP) server to every new network node.

32. Dynamic IP addresses are generally implemented by Internet service providers and networks that have a large number of connecting clients or end-nodes. Unlike static IP addresses, dynamic IP addresses are not permanent. A dynamic IP is assigned to a node until it's connected to the network; therefore, the same node may have a different IP address every time it reconnects with the network.

33. I know through training and experience that T-Mobile is able to "resolve" associated Dynamic IP addresses. When T-Mobile "resolves" those IP

addresses, they are able to identify the associated user and the specific cellular phone associated with that user. In other words, when T-Mobile is provided with a particular associated IP address and time stamp (like the IP address and time stamp described here), T-Mobile is able to (i) determine the particular cellular phone that used that IP address; and (ii) collect cell-site location data associated with that same particular cellular phone, in the manner described below.

TECHNICAL BACKGROUND: CELL SITE LOCATION DATA

34. In my training and experience, I have learned that the Service Provider is a company that provides cellular communications service to the general public. I also know that providers of cellular communications service have technical capabilities that allow them to collect and generate information about the locations of the cellular devices to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular device and, in some cases, the "sector" (i.e., faces of the towers) to which the device connected. These towers are often a half- mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate general location of the cellular device.

35. Based on my training and experience, I know that the Service Provider can collect cell-site data on a prospective basis about the Target Cell Phone. Based on my training and experience, I know that for each communication a cellular device

makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer was connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as the Service Provider typically collect and retain cell-site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

36. I know that some providers of cellular telephone service have technical capabilities that allow them to collect and generate E-911 Phase II data, also known as GPS data or latitude-longitude data. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. As discussed above, cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data is typically less precise that E-911 Phase II data. Based on my training and experience, I know that the Service Provider can collect E-911 Phase II data about the location of the Target Cell Phone, including by initiating a signal to determine the location of the

Target Cell Phone on the Service Provider's network or with such other reference points as may be reasonably available.

37. Based on my training and experience, I know each cellular device has one or more unique identifiers embedded inside it. Depending on the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), a Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Equipment Identity ("IMEI"). The unique identifiers – as transmitted from a cellular device to a cellular antenna or tower – can be recorded by pen-trap devices and indicate the identity of the cellular device making the communication without revealing the communication's content.

38. Based on my training and experience, I know that wireless providers such as the Service Provider typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless communication service. I also know that wireless providers such as the Service Provider typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular device and other transactional records, in their normal course of business. In my training and experience, this

information may constitute evidence of the crimes under investigation because the information can be used to identify the Target Cell Phone's user or users and may assist in the identification of co-conspirators and/or victims.

39. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

40. I further request that the Court direct the Service Provider to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control.

41. I also request that the Court direct the Service Provider to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with the Service Provider's services, including by initiating a signal to determine the location of the Target Cell Phone on the Service Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate the Service Provider for reasonable expenses incurred in furnishing such facilities or assistance.

42. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 90 days after the collection authorized by the warrant has been completed. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the Target Cell Phone

would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

43. Because the warrant will be served on the Service Provider, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the Target Cell Phone outside of daytime hours.

ATTACHMENT A

Property to Be Searched

1. Records and information associated with the cellular device assigned IP Address 2607:fb90:d222:4d8d:b933:527f:26c3:698f, used at the following dates and times:

- Time 2021-06-08 15:20:39 UTC
- Time 2021-06-08 15:20:18 UTC
- Time 2021-06-08 15:19:42 UTC
- Time 2021-06-08 15:18:52 UTC
- Time 2021-06-08 15:18:44 UTC
- Time 2021-06-08 14:11:27 UTC
- Time 2021-06-08 14:09:13 UTC
- Time 2021-06-08 14:11:27 UTC
- Time 2021-06-08 14:09:13 UTC
- Time 2021-06-08 13:43:40 UTC
- Time 2021-06-08 13:43:16 UTC
- Time 2021-06-08 13:42:35 UTC
- Time 2021-06-08 13:42:30 UTC
- Time 2021-06-08 13:41:10 UTC
- Time 2021-06-08 13:23:13 UTC
- Time 2021-06-08 13:20:06 UTC
- Time 2021-06-08 13:17:22 UTC

(referred to herein and in Attachment B as "the Target Cell Phone"), that is in the custody or control of T-Mobile (referred to herein and in Attachment B as the "Service Provider"), a wireless communications service provider that is headquartered at 4 Sylvan, Parsippany, NJ 07054

2. The Target Cell Phone.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Service Provider, including any information that has been deleted but is still available to the Service Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Service Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A:

a. The following subscriber and historical information about the customers or subscribers associated with the Target Cell Phone for the time period of May 9, 2021, to the date of this warrant's execution:

   i. Names (including subscriber names, user names, and screen names);

   ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

   iii. Local and long distance telephone connection records;

   iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

   v. Length of service (including start date) and types of service used;

   vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

ix. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Target Cell Phone, including:

(A) the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

(ii) information regarding the cell tower and antenna face (also known as "sectors" through which the communications were sent and received) as well as per-call measurement data (also known as "real-time tool" or "RTT").

b. Information associated with each communication to and from the Target Cell Phone for a period of 30 days from the date of this warrant, including:

i. Any unique identifiers associated with the cellular device, including ESN, MEIN, MSISDN, IMSI, SIM, or MIN;

ii. Source and destination telephone numbers;

iii. Date, time, and duration of communication; and

iv. All data about the cell towers (i.e. antenna towers covering specific geographic areas) and sectors (i.e. faces of the towers) to which the Target Cell Phone will connect at the beginning and end of each communication as well as per-call measurement data (also known as "real-time tool" or "RTT").

c. Information about the location of the Target Cell Phone for a period of 30 days, during all times of day and night. "Information about the location of the Target Phone" includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information.

i. To the extent that the information described in the previous

paragraph (hereinafter, "Location Information") is within the possession, custody, or control of the Service Provider, the Service Provider is required to disclose the Location Information to the government. In addition, the Service Provider must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with the Service Provider's services, including by initiating a signal to determine the location of the Target Cell Phone on the Service Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate the Service Provider for reasonable expenses incurred in furnishing such facilities or assistance.

ii. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

II. Information to be Seized by the Government

All information described above in Section I that constitutes fruits, evidence and instrumentalities relating to a violation of 18 U.S.C. § 1073 (Unlawful Flight to Avoid Prosecution) involving PENA-GOMEZ, since August 10, 2020.

All information described above in Section I that will assist in arresting PENA-GOMEZ, who was charged on March 5, 2021, with violating 18 U.S.C. § 1073, and who is the subject of an arrest warrant issued on March 5, 2021, and is a "person to be arrested" within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records

produced by the Service Provider in order to locate the things particularly described in this Warrant.